Energy Efficient Operation Cycle Determination Scheme of Fuzzy Based IHA in Air Purification IoT

Ye-lim Kang, Tae-ho Cho

Abstract: ***Fine dust is a harmful particulate substance floating in the air and is divided into PM10 (which is 10 um in diameter or less) and PM2.5 (which is 2.5 um in diameter or less). Fine dust is a major cause of chronic respiratory diseases, which may occur naturally through forest fires or yellow dust, but it is mainly caused by combustion of fossil fuels such as oil and coal, or by automobile exhaust gases. When this type of bad outdoor fine dust flows into buildings, the indoor air becomes polluted, making it easier for workers or students who spend a lot of time indoors to be at risk for chronic respiratory diseases. To minimize this risk, recent research and development has focused on systems to purify indoor air by filtering fine dust. In this paper, we introduce a Wireless Sensor Networks (WSNs)-based Internet of Things (IoT) air purification system. In the WSNs-based IoT air purification system, it is important to maintain the integrity of the sensing data because the IoT air purifier operates based on the sensing data detected by sensor nodes. To defend the IoT air purifier against false report injection attacks, the existing fuzzy-based Interleaved Hop-by-Hop Authentication (IHA) detects false report injection attacks through Data Calibration. In addition to the existing fuzzy-based IHA sets, the security limit changes according to the network situation using fuzzy logic and adjusts the security and energy. However, the existing fuzzy-based IHA executes a fuzzy system every time it detects a normal event or false report injection attack, which requires additional message overhead and increases the transmission/reception energy, which increases the energy burden of the sensor nodes. To address this problem, we propose a method to control the operation cycle of the fuzzy system using the evaluation function. This proposed method has the advantage that the trade-off relationship between energy and security can be appropriately used to adjust the operation cycle and increase the lifetime of the network.***

Keywords : Network Security, Internet of Things, Wireless Sensor Networks, Interleaved Hop-by-hop Authentication, False report injection attack

I. INTRODUCTION

Fine dust is particulate matter in the atmosphere with a diameter of 10 um or less [1]. Fine dust is caused by natural phenomena or combustion of fossil fuel, and smaller particles are more harmful to the human body. Fine dust is the main cause of chronic respiratory disease and may exacerbate both respiratory symptoms and lung function when people with chronic respiratory disease are exposed to fine dust for a long time. When outdoor fine dust flows into a building, the quality of the indoor air also deteriorates. Office workers and students spend most of their time indoors and fine dust can be detrimental to these people. Recently, there have been many systems developed to purify indoor air by filtering fine dust. In this paper, we introduce an indoor air purification system using a WSNs-based IoT. A WSNs is a wireless network composed of hundreds to thousands of sensor nodes and a Base Station (BS) [2]. This is a good system that can be applied to natural phenomena covering a large area at low cost or for real time monitoring. Because IoT communicates through the Internet using embedded sensors and communication modules, it can provide various services to users and can be applied to various fields such as healthcare, home [3-4]. The system to use WSNs and IoT is WSNs-based IoT system. In a WSNs-based IoT system, the sensor nodes detect an event that occurs and generate an event report, which is transmitted to the IoT device through the BS. The IoT device receiving the event report determines whether to execute an operation based on the event information detected by the sensor nodes. Therefore, it is important to maintain the integrity of the sensing data because the IoT device executes normal operation when the sensing data values detected by sensor nodes are normal. However, it is difficult to maintain the integrity of the sensing data if a false report injection attack occurs. In the existing fuzzy-based IHA, security and energy are flexibly adjusted by dynamically determining the security limit according to the network situation using the fuzzy system [5]. The security limit is determined by the security threshold used in IHA and is the number of the Message Authentication Code (MAC) included in the event report, which is a security index in WSNs [6-7]. A trade-off relationship exists in that the security improves when the security threshold increases, but the energy of sensor nodes is unnecessarily consumed, while security decreases when the security threshold decreases, but the energy of sensor nodes is saved. The existing fuzzy-based IHA adjusts security and energy in consideration of this trade-off. However, the operation cycle of the fuzzy system is not considered because the fuzzy system is executed every time a normal event or a false report injection attack occurs, resulting in frequent additional message overhead requesting information to the sensor node and increased usage of transmission/reception energy of the sensor node.

Revised Manuscript Received on July 30, 2020.
***** Correspondence Author
Ye-lim Kang, Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea. Email:missye7322@skku.edu
Tae-ho Cho*, Department of Computer Science and Engineering, Sungkyunkwan University, Suwon, Republic of Korea. Email: thcho@skku.edu

To address this, we propose a method in this paper to update the operation cycle of the fuzzy system according to the network situation using an evaluation function. Since the proposed scheme controls the operation cycle of the fuzzy system using the evaluation function, the transmission/reception energy of the sensor node decreases, thereby increasing the overall network lifetime.

The content of this paper is as follows. Chapter 2 of this paper describes the false report injection attack, IHA, IoT, WSNs-based IoT, and fuzzy logic, and Chapter 3 describes the proposed scheme. Chapter 4 explains the experimental results, and finally Chapter 5 provides a conclusion.

II. RELATED WORK

A. False report injection attack

A false report injection attack occurs when an attacker generates a false report using keys obtained by compromising sensor nodes and then injects the false report into the network [8]. Typically, when sensor nodes detect normal events that actually occur, they generate event reports that are transmitted to the BS. Then, the BS can provide the users with a useful service using the normal event report. On the other hand, a false report is a report that the attacker falsely generates about the event that has not occurred. When a false report is injected into the network, the limited energy of sensor nodes is excessively consumed during transmission of the false report. In addition, when a false report arrives at the BS, there is a problem in that the false report may lead the BS to provide users with the wrong service. To defend against this, there are WSNs security protocols such as IHA where the sensor node and BS detect false reports using MAC.

B. Interleaved Hop-by-Hop Authentication (IHA)

IHA is a security protocol that allows the sensor nodes and BS to detect false reports using MAC if the number of compromised sensor nodes does not exceed the security threshold. IHA operates in the order of Node Initialization and Deployment, Association Discovery, Report Endorsement, En-route Filtering, and BS verification. First, in the Node Initialization and Deployment phase, the key server preloads individual keys to all sensor nodes, and each sensor nodes generates an authentication key using a preloaded individual key. Second, in the Association Discovery phase, BS hello and Cluster Acknowledgement are performed to initially set association nodes of each sensor node. In BS hello, each sensor node discovers the upper association node at the (security threshold+1) hop. In Cluster Acknowledgement, each sensor node discovers the lower association node at the (security threshold+1) hop. Third, in the Report Endorsement phase, if a normal event occurs, the sensor nodes detect an event and generate an event report containing MAC. Fourth, in the En-route Filtering phase, a sensor node receiving the event report checks if the number of pairwise MAC included in the event report is correct after verifying the authenticity of the event report using a key shared with a child node on one hop. At this time, if the number of the pairwise MAC is correct, the sensor node verifies the pairwise MAC in the event report using the pairwise key shared with the lower association node, and the verified MAC is removed from the event report. The sensor node then generates a MAC using the pairwise key shared with the upper association node and adds it to the event report and retransmits it. Finally, in the BS verification phase, when the event report arrives at the BS, and the BS verifies the MAC using the individual keys. If the verification succeeds, the BS approves the event report. Conversely, the corresponding event report is dropped if verification fails.

C. Security threshold of IHA

The security threshold of IHA represents the security of WSNs and indicates the number of MAC included in the event report. The network's security strength depends on the security threshold of IHA that the network administrator sets, which is related to the overall network lifetime and energy efficiency. In general, if the security threshold increases, the number of MAC increases and the verification count of the event report increases, thereby enhancing security. However, there is a problem in that the network lifetime decreases because the size of the event report increases, and the transmission/reception energy of sensor nodes increases. On the other hand, if the security threshold decreases, the number of MAC decreases, and the verification count of the event report decreases, so there is a problem in that security is weakened. However, the network lifetime increases because the size of the event report decreases and the transmission/reception energy of sensor nodes decreases. Therefore, it is important to dynamically adjust the security threshold according to the network situation because the security threshold and network lifetime are in a trade-off relationship.

D. Internet of Things (IoT)

IoT is a technology in which objects in everyday life such as refrigerators, smartphones, and cameras are connected through the Internet. Things connected through the Internet by embedding sensors and wireless communication modules are called IoT devices, and these things can exchange various types of data by interacting through wireless communication. In addition, IoT has the advantage of detecting various situation through sensors while using the internet. Thus, the detected event information can be used in various fields such as home appliances and healthcare through big data analysis. In particular, IoT is widely used in systems that purify indoor air by detecting fine dust.

E. Wireless Sensor Network (WSNs)-based Internet of Things (IoT)

WSNs-based IoT is a system that combines WSNs and IoT. If a sensor node detects an event occurring in real time, an event report is generated and is transmitted into the IoT device through the BS. The IoT device can both determine whether to execute the operation of the IoT device based on the received event information and accumulate the event information to provide users with the service in the future. Also, it can be used to prevent the execution of abnormal operation of the IoT device due to the false report injection attack.

The WSNs-based IoT system has the advantage of being able to monitor real-time phenomena over a wide area at low cost and to provide users with various services based on the collected event information.

F. Fuzzy Logic

Fuzzy logic, does not just divide information into either 0 or 1 like a computer but deals with the ambiguous logic between 0 and 1 in the real world [9-10]. An example is a sentence such as 'If the height is about 170cm, is a person smaller or larger?' Since height is different for each person, the answer is ambiguous and fuzzy logic determines the degree of ambiguity. First, the fuzzy set is defined, and input values are converted to the corresponding membership function values through fuzzification. Then, several rules about each input value are checked. Finally, inference values from checked rules are converted to correct values through defuzzification. Mamdani's inference method is used in the inference scheme and the Center of Gravity Method is used in the defuzzification [11].

III. PROPOSED SCHEME

A. Problem Statement

In the existing fuzzy-based IHA, a fuzzy system is used to set a security threshold considering energy and security for each cluster. The existing fuzzy-based IHA has the advantage that it can properly adjust energy and security by dynamically outputting the security threshold according to the network situation through fuzzy rules. However, since the operation cycle of the fuzzy system is not considered, the fuzzy system is executed too many times so additional message overhead is generated for obtaining input values of the fuzzy system. Therefore, as the fuzzy system is executed more frequently, additional message overhead increases, which decreases overall network lifetime and cannot properly adjust security. To solve this problem, we propose the method to determine a proper fuzzy system operation cycle using an evaluation function.

B. Assumption

Data Calibration must be performed to determine the correct operation execution of the IoT air purifier [12]. For Data Calibration, we assume that there is a sufficient amount of normal data in the IoT air purifier.

C. Proposed scheme

I. Evaluation Function

$$FLOC(p) = \left(\frac{1}{REN(p)} + \frac{1}{HC(p)}\right) \times 100 \quad (1)$$

The Fuzzy Logic Operation Cycle (FLOC) is determined by considering the Remaining Energy of the Node (REN) and Hop Count (HC). As REN and HC increase, FLOC increases, and FLOC decreases as REN and HC decrease. A higher FLOC results in more frequently information requests to the sensor node to obtain input values for the fuzzy system. Thus, the energy of the sensor node is unnecessarily consumed, and the security strength can be updated frequently, thereby enhancing security. Conversely, a lower FLOC results in less information requested to the sensor node to obtain input values of the fuzzy system, so the energy of the sensor node is consumed a little, and the security strength cannot be updated frequently, thereby weakening security.

II. Operation process

Fig. 1 shows the operation process when a normal event

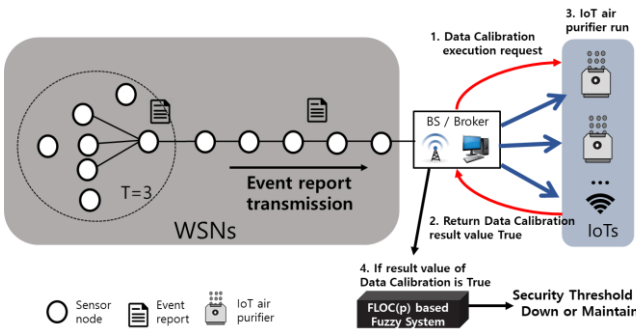

Fig. 1. Operation process when a normal event occurs

occurs. If a normal event occurs, WSNs and the IoT air purifier detect the event at the same time. Sensor nodes generate the event report, and it is transmitted to the BS. The BS receiving the event report requests the execution of Data Calibration to the IoT air purifier and the IoT air purifier compares the sensing data value of WSNs with the sensing data value of IoT through Data Calibration. Since the compared sensing data value is within a preset error range, the IoT air purifier judges that a normal event occurred, the result value of Data Calibration returns 'true', and the result value of Data Calibration is transmitted to the BS. Then, the IoT air purifier executes normal operation. If the result value of Data Calibration is 'true', the BS executes the fuzzy system by the operation cycle set by the network administrator initially and the security threshold is "down" or "maintain". Finally, the operation cycle of the fuzzy system is updated considering the remaining energy and the number of hops of the cluster in which the event occurred by the evaluation function. Thereafter, the fuzzy system is operated by the operation cycle updated by the evaluation function.

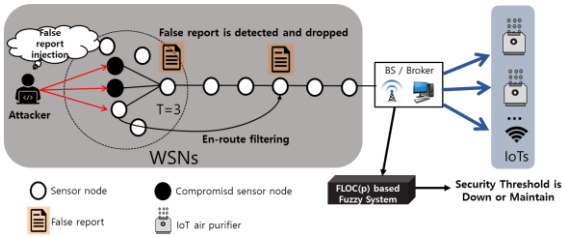

Fig. 2. Operation process in a false report injection attack situation where the number of compromised sensor nodes is below the security threshold

Fig. 2 shows operation process in a false report injection attack situation where the number of compromised sensor nodes is below the security threshold. If a false report injection attack occurs in which the number of compromised sensor nodes is below security threshold, the false report is dropped by En-route filtering of IHA, and BS executes the fuzzy system.

The fuzzy system is initially executed by the operation cycle set by the network administrator, and the security threshold is "down" or "maintain". Finally, the operation cycle of the fuzzy system is updated considering the remaining energy and the number of hops of the cluster in which the attack occurred by the evaluation function. Thereafter, the fuzzy system is operated by the operation cycle updated by the evaluation function.

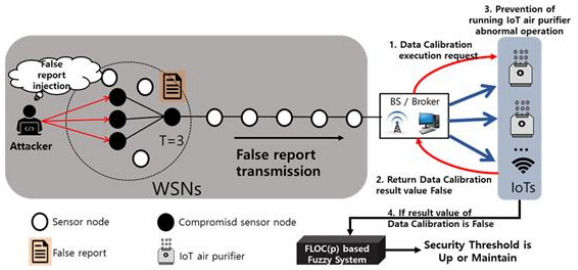

Fig 3. Operation process in a false report injection attack situation where the number of compromised sensor nodes exceeds the security threshold

Fig. 3 shows operation process in a false report injection attack situation where the number of compromised sensor nodes exceeds the security threshold. If a false report injection attack occurs such that the number of compromised sensor nodes exceeds security threshold, the false report is transmitted to the BS. The BS receiving the false report requests the execution of Data Calibration to the IoT air purifier, and the IoT air purifier compares the sensing data value of WSNs with the sensing data value of the IoT through Data Calibration. Since the compared sensing data value is not within the preset error range, the IoT air purifier judges that a false report injection attack occurred, and the result value of Data Calibration returns 'false'. Then, the result value of Data Calibration is transmitted to the BS. In addition, the IoT air purifier prevents abnormal operation because the result of Data Calibration is 'false'. If the result of Data Calibration is 'false', the fuzzy system of BS is not executed. Instead, the IoT air purifier initially executes the fuzzy system by the operation cycle set by the network administrator, so the security threshold is "up" or "maintain". Finally, the operation cycle of the fuzzy system is updated considering the remaining energy and the number of hops of the cluster in which the attack occurred by the evaluation function. After that, the fuzzy system is operated by the operation cycle updated by the evaluation function.

IV. PERFORMANCE EVALUATION

A. Experimental environment

Table- I: Experimental environment

Parameter	Value
Field Size	1000 m x 1000 m
Cluster Size	50m x 50m
Number of Nodes	2000
Number of Cluster Head Nodes	400
MAC Size	1 byte
Energy Consumption of Transmitting [13]	16.25 (per 1byte)
Energy consumption of receiving	12.5 (per 1byte)
Energy Consumption of Report Generation	70
Energy Consumption of MAC Generation	15
Energy Consumption of MAC Verification	75
Security Threshold	2-4
Energy of Sensor node	2 J
Information Request Message of Sensor Node	2 bytes
En-route Filtering Notification Message of Sensor Node	2 bytes

B. Experiment results

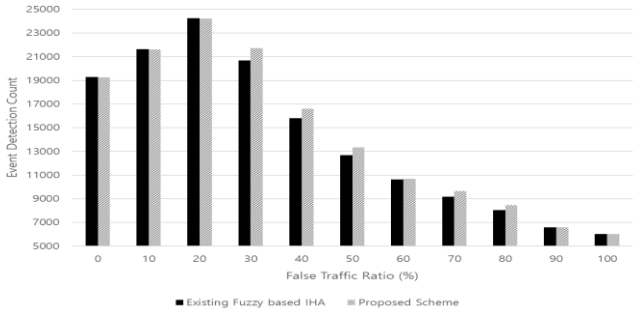

Fig. 4. Event Detection Count according to FTR

Fig. 4 shows the event detection count according to FTR, which is an indicator of the duration of the network. To compare the existing fuzzy-based IHA with the proposed scheme, we generated an event at a random position until even one of the 2,000 sensor nodes had less than 10% remaining energy. Then, we analyzed the event detection count according to the FTR. When the FTR is 0-20%, the event detection count gradually increases, and then gradually decreases from 30-100%. The existing fuzzy-based IHA executes a fuzzy system each time the BS or IoT air purifier detects a normal event or false report injection attack, which generates additional message overhead for obtaining input values of the fuzzy system. However, even if the BS and IoT air purifiers detect normal events or false report injection attacks in the proposed scheme, the fuzzy system is not executed if it has not reached the fuzzy system's operation cycle. So, additional message overhead can be reduced compared to the existing fuzzy-based IHA. This saves sensor node energy, thus improving network lifetime in the proposed scheme. Therefore, the proposed scheme shows an average network extension rate of 2.368% over the existing fuzzy-based IHA.

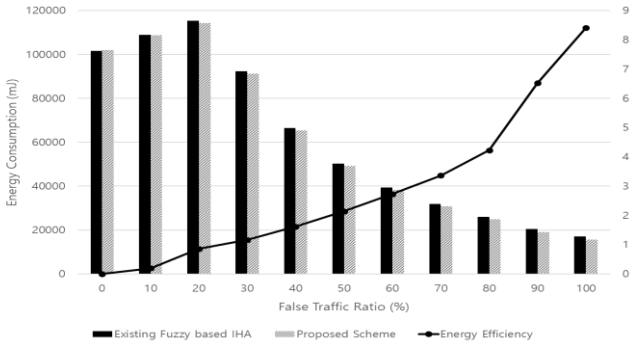

Fig. 5. Energy Consumption and Energy Efficiency according to FTR

Fig. 5 shows the overall energy consumption and energy efficiency according to the FTR. To compare the existing fuzzy-based IHA with the proposed scheme, we generated 6019~21591 events at random positions and analyzed the overall energy consumption according to the FTR. When the FTR is 0-20%, the energy consumption gradually increases, and then gradually decreases from 30-100%. This shows that the energy efficiency increases as FTR increases. In the existing fuzzy-based IHA, the BS and IoT air purifier do not consider the overall situation of the network (the remaining energy of the sensor node and the number of hops). Thus, the fuzzy system is executed too often to update the security strength frequently, so the security is enhanced. However, since information requests for the input values of the fuzzy system are frequently generated, a large amount of energy is consumed as transmission/reception energy. Conversely, in the proposed scheme, the BS and IoT air purifier execute the fuzzy system by the operation cycle of evaluation function, so the security strength update frequency is reduced compared to the existing fuzzy-based IHA, which may weaken the security but save transmission and reception energy. Therefore, in the proposed scheme, an energy efficiency improvement of up to 8.416% was observed compared to the existing fuzzy-based IHA.

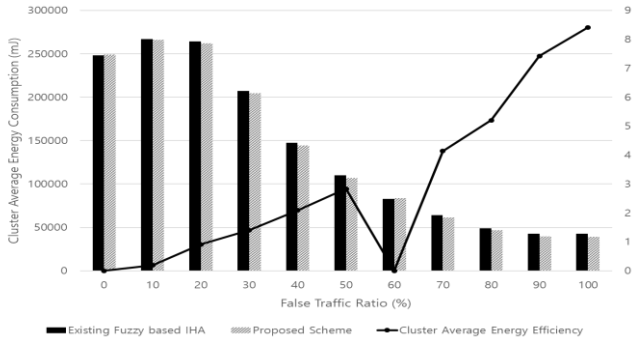

Fig. 6. Cluster Average Energy Consumption and Energy Efficiency according to FTR

Fig. 6 shows the cluster average energy consumption and energy efficiency according to FTR. To compare the existing fuzzy-based IHA with the proposed scheme, we generated 6019-21591 events at random positions and analyzed the average energy consumption of each cluster according to FTR. When the FTR is 0-10%, the average energy consumption per cluster increased gradually, then decreased from 20-100%. The reason why the energy consumption decreased as the FTR increased is because the false reports were dropped by En-route filtering and did not reach the BS, thus saving the transmission/reception and verification energy of the sensor node. The existing fuzzy-based IHA executed the fuzzy system every time without considering the operation cycle, and the proposed scheme reduces the number of security strength updates because the fuzzy system is executed by the evaluation function considering the remaining energy and hop count. Therefore, in the proposed scheme, an energy efficiency improvement of up to 8.417% was observed compared to the existing fuzzy-based IHA.

V. CONCLUSION

In the existing fuzzy-based IHA, the situation that the security is strengthened or the energy needs to be saved is recognized through the fuzzy rule. The security threshold is adjusted according to the result. This is important because the lifetime and security of the network are directly related to the security threshold. However, the existing fuzzy-based IHA does not take into account the operation cycle of the fuzzy system, so it executes the fuzzy system every time a normal event or attack occurs, resulting in additional message overhead and increased transmission/reception energy, which consumes the limited energy of the sensor node. Thus, the overall network lifetime is reduced. To execute the fuzzy system considering the trade-off between security and network lifetime, it is important to consider the operation cycle of the fuzzy system. Therefore, we proposed a method to find an appropriate operation cycle suitable for the network situation by the evaluation function. If the operation cycle of the fuzzy system is high, energy is consumed by executing the fuzzy system too often. Thus, network lifetime is reduced, but security is strengthened by frequently updating the security strength. In contrast, if the operation cycle of the fuzzy system is low, the fuzzy system is not run as often, which consumes less energy, thereby increasing the network lifetime, but the security is weakened because the security strength is not frequently updated. In conclusion, it is possible to flexibly control the execution of the fuzzy system according to the network situation through the evaluation function, as well as efficiently manage the security and network lifetime. Therefore, it is much more efficient in terms of energy compared to the existing fuzzy-based IHA.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. NRF-2018R1D1A1B07048961)

REFERENCES

1. Kang, Dongmug, and Jong-Eun Kim. "Fine, ultrafine, and yellow dust: emerging health problems in Korea." Journal of Korean medical science 29.5 (2014): 621-622.
2. Akyildiz, Ian F., et al. "A survey on sensor networks." IEEE Communications magazine 40.8 (2002): 102-114.
3. Al-Fuqaha, Ala, et al. "Internet of things: A survey on enabling technologies, protocols, and applications." IEEE communications surveys & tutorials 17.4 (2015): 2347-2376.
4. Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.
5. Ye-lim Kang and Tae-ho Cho. "Fuzzy-based Dynamic Security Parameters Determination Method to Improve Energy Efficiency." International Journal of Engineering and Advanced Technology (IJEAT) 9.4 (2020):1952-1958.
6. Zhu, Sencun, et al. "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks." IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004. IEEE, 2004.
7. Zhu, Sencun, et al. "Interleaved hop-by-hop authentication against false data injection attacks in sensor networks." ACM Transactions on Sensor Networks (TOSN) 3.3 (2007): 14-es.
8. Jeba, S. Annlin, and B. Paramasivan. "False data injection attack and its countermeasures in wireless sensor networks." European Journal of Scientific Research 82.2 (2012): 248-257.

9. Zadeh, Lotfi Asker. "Fuzzy sets as a basis for a theory of possibility." Fuzzy sets and systems 1.1 (1978): 3-28.
10. Lee, Chuen-Chien. "Fuzzy logic in control systems: fuzzy logic controller. II." IEEE Transactions on systems, man, and cybernetics 20.2 (1990): 419-435.
11. Mamdani, Ebrahim H., and Sedrak Assilian. "An experiment in linguistic synthesis with a fuzzy logic controller." International journal of man-machine studies 7.1 (1975): 1-13.
12. Ye-lim Kang and Tae-ho Cho. “Detection of False Report Injection At Wsns Based on Data Calibration in Iot Environment.” International Journal of Recent Technology and Engineering (IJRTE) 8.4 (2019): 8956-8960.
13. Ye, Fan, et al. "Statistical en-route filtering of injected false data in sensor networks." IEEE Journal on Selected Areas in Communications 23.4 (2005): 839-850.

AUTHORS PROFILE

Ye Lim Kang received her B.S. degree in Information and Communication Engineering from Sungkyul University, Korea, in February 2018. She is currently a master student in the Information and Communication Engineering at Sungkyunkwan University, Korea. Her research interests include internet of things, artificial intelligence, wireless sensor network and network security.

Tae Ho Cho received his Ph.D. in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and B.S. and M.S. degrees in Electrical Engineering from Sungkyunkwan University, Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the College of Computing at Sungkyunkwan University, Korea. His research interests include wireless sensor networks, intelligent systems, modeling and simulation, and enterprise resource planning.